文部科学省後援

情報システム試験

平成26年度前期 情報検定

＜実施　平成26年9月14日（日）＞

システムデザインスキル

（説明時間　14：30～14：40）

（試験時間　14：40～16：10）

・試験問題は試験開始の合図があるまで開かないでください。

・解答用紙（マークシート）への必要事項の記入は，試験開始の合図と同時に行いますので，それまで伏せておいてください。
・試験開始の合図の後，次のページを開いてください。**＜受験上の注意＞**が記載されています。必ず目を通してから解答を始めてください。
・試験問題は，すべてマークシート方式です。正解と思われるものを１つ選び，解答欄の０をＨＢの黒鉛筆でぬりつぶしてください。２つ以上ぬりつぶすと，不正解になります。
・辞書，参考書類の使用および筆記用具の貸し借りは一切禁止です。
・電卓の使用が認められます。ただし，下記の機種については使用が認められません。

＜使用を認めない電卓＞

１．電池式（太陽電池を含む）以外の電卓
２．文字表示領域が複数行ある電卓（計算状態表示の一行は含まない）
３．プログラムを組み込む機能がある電卓
４．電卓が主たる機能ではないもの
　＊パソコン（電子メール専用機等を含む），携帯電話（ＰＨＳ），スマートフォン，タブレット，電子手帳，電子メモ，電子辞書，翻訳機能付き電卓，音声応答のある電卓，電卓付腕時計等
５．その他試験監督者が不適切と認めるもの

一般財団法人　職業教育・キャリア教育財団

＜受験上の注意＞

１．この試験問題は17ページあります。ページ数を確認してください。
乱丁等がある場合は，手をあげて試験監督者に合図してください。
※問題を読みやすくするために空白ページを設けている場合があります。

２．解答用紙（マークシート）に，受験者氏名・受験番号を記入し，受験番号下欄の数字をぬりつぶしてください。正しく記入されていない場合は，採点されませんので十分注意してください。

３．試験問題についての質問には，一切答えられません。自分で判断して解答してください。

４．試験中の筆記用具の貸し借りは一切禁止します。筆記用具が破損等により使用不能となった場合は，手をあげて試験監督者に合図してください。

５．試験を開始してから30分以内は途中退出できません。30分経過後退出する場合は，もう一度，受験番号・マーク・氏名が記載されているか確認して退出してください。なお，試験終了５分前の合図以降は退出できません。試験問題は各自お持ち帰りください。

６．試験後にお知らせする合否結果（合否通知），および合格者に交付する「合格証・認定証」はすべて，Ｗｅｂページ（ＰＣ，モバイル）での認証によるデジタル「合否通知」，デジタル「合格証・認定証」に移行しました。
①団体宛にはこれまでと同様に合否結果一覧ほか，試験結果資料一式を送付します。
②合否等の結果についての電話・手紙等でのお問い合わせには，一切応じられませんので，ご了承ください。

問題を読みやすくするために,
このページは空白にしてあります。

問題１　次の経営戦略に関する記述を読み，各設問に答えよ。

経営戦略とは，外部環境の変化に適応しながら，他企業との競争に勝ち抜いていくための方針を，経営理念やビジョンにもとづき決定することである。

経営戦略を策定するうえでさまざまな調査・分析技法を駆使し，現状を把握する必要がある。

＜設問１＞　次の SWOT 分析に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

企業内外の環境を分析し，その結果を分類・整理する手法として SWOT 分析がある。［(1)］を「機会と脅威」，［(2)］を「強みと弱み」に分類し，自組織と競合他社について分析する手法である。［(1)］とはその企業や組織だけでは変えることが不可能なものであり，［(2)］とはその組織内で改善することができるものである。

分析の結果，［(3)］は，追い風に乗って積極的な戦略を採ることが有効であり，［(4)］は，防衛策を図るか撤退するかなどの判断をする。

		(1)	
		機会	脅威
(2)	強み	a	b
	弱み	c	d

図１　SWOT 分析

(1)，(2) の解答群

ア．外部要因　　イ．技術要因　　ウ．経済要因
エ．資源要因　　オ．市場要因　　カ．内部要因

(3)，(4) の解答群

ア．a　　イ．b　　ウ．c　　エ．d

＜設問２＞　次の PPM 分析に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

市場の成長率と自社製品の市場占有率から自社製品の市場におけるポジションを分析する手法に PPM（プロダクトポートフォリオマネジメント）がある。

PPM では，図２のように，４つの事象に事業を分類する。

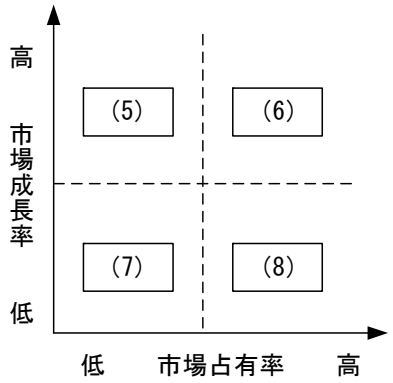


図２　PPM 図

［(5)］ … 成長市場であるのに売れていない。大きな投資を行うことによって［(6)］になる可能性があるもの。

［(6)］ … 成長市場であるため，常に新しい投資が必要となり，資金を生み出す効果はそれほど大きくないが，いずれ［(8)］になる可能性があるもの。

［(7)］ … 将来性もなく，資金を生み出す効果もないため，将来性には撤退を考える必要があるもの。

［(8)］ … 市場成長率が低いので投資は少なくてすみ，高いシェアを持つため，資金を生み出す効果を大きく期待できるもの。

(5) ～ (8) の解答群

ア．金のなる木　　イ．花形

ウ．負け犬　　エ．問題児

問題２　次のコンピュータシステムの評価に関する記述を読み，各設問に答えよ。

＜設問１＞　次の RASIS に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

コンピュータシステムの評価指標として，RASIS がある。

表１　RASIS

Reliability （信頼性）	システムに要求される機能を安定して提供できることである。これを評価する指標の一つとして，故障と故障の間の平均時間である［(1)］がある。
Availability （可用性）	システムを適時に利用することができることである。これを評価する指標の一つとして稼働率がある。
Serviceability （保守性）	システムに障害や故障が発生したときに，原因の発見や復旧がしやすいことである。これを評価する指標の一つとして［(2)］がある。
Integrity （［(3)］）	システムで扱う情報が常に正しい状態を保っているかということである。
Security （［(4)］）	システムへ外部からの不正侵入や情報の改ざんなど，不正アクセスがされにくいことである。

(1)，(2) の解答群

ア．FIT　　イ．IOPS　　ウ．MTBF　　エ．MTTR

(3)，(4) の解答群

ア．拡張性　　イ．機密性　　ウ．冗長性　　エ．保全性

＜設問２＞　次の可用性に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

可用性を示す指標の一つとして稼働率がある。システムは，正常に稼働している時間と障害復旧(修理)している時間を一つのサイクルとして運用している。稼働率は，運用中のサイクルの中で，システムが稼働している時間の割合を表す。例えば図１の場合，システムが稼働している平均時間が［(5)］時間，障害を取り除くための平均時間が［(6)］時間となり，稼働率は［(7)］となる。

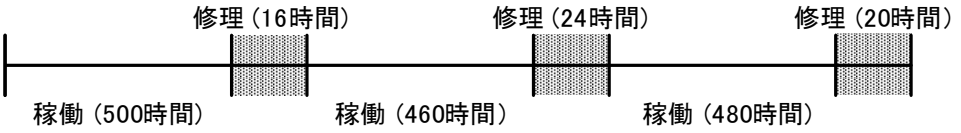


図１　システムの稼働状況

障害が発生したとしても，システムの機能全体を停止させないために，冗長なシステムを用意する考え方がある。図２のような装置構成で，少なくともどちらか一方が稼働していれば，システムの機能が停止しない場合，システムの稼働率は［(8)］となる。

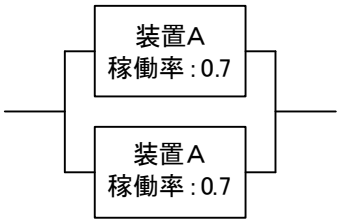


図２　装置構成１

(5)，(6) の解答群

ア．16	イ．20	ウ．24	エ．28
オ．440	カ．460	キ．480	ク．500

(7)，(8) の解答群

ア．0.49	イ．0.68	ウ．0.78	エ．0.86
オ．0.91	カ．0.94	キ．0.96	ク．0.99

＜設問３＞　次の並列化に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

図３の機器構成における全体の稼働率は［　(9)　］である。これを 0.85 以上に向上させるために装置を並列化したい。並列化には各装置の購入などのコストが発生するため，このコストを最低限にする必要がある。各装置の稼働率と追加のためのコストを表２に示す。稼働率が 0.85 以上で最小のコストで済む並列化は［　(10)　］である。

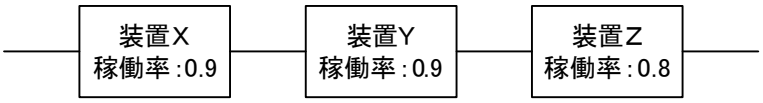


図３　装置構成２

表２　各装置の稼働率およびコスト

	装置単体での稼働率	購入コスト(単位：万円)
装置Ｘ	0.9	80
装置Ｙ	0.9	90
装置Ｚ	0.8	100

(9) の解答群

ア．0.512　　イ．0.576　　ウ．0.648　　エ．0.729

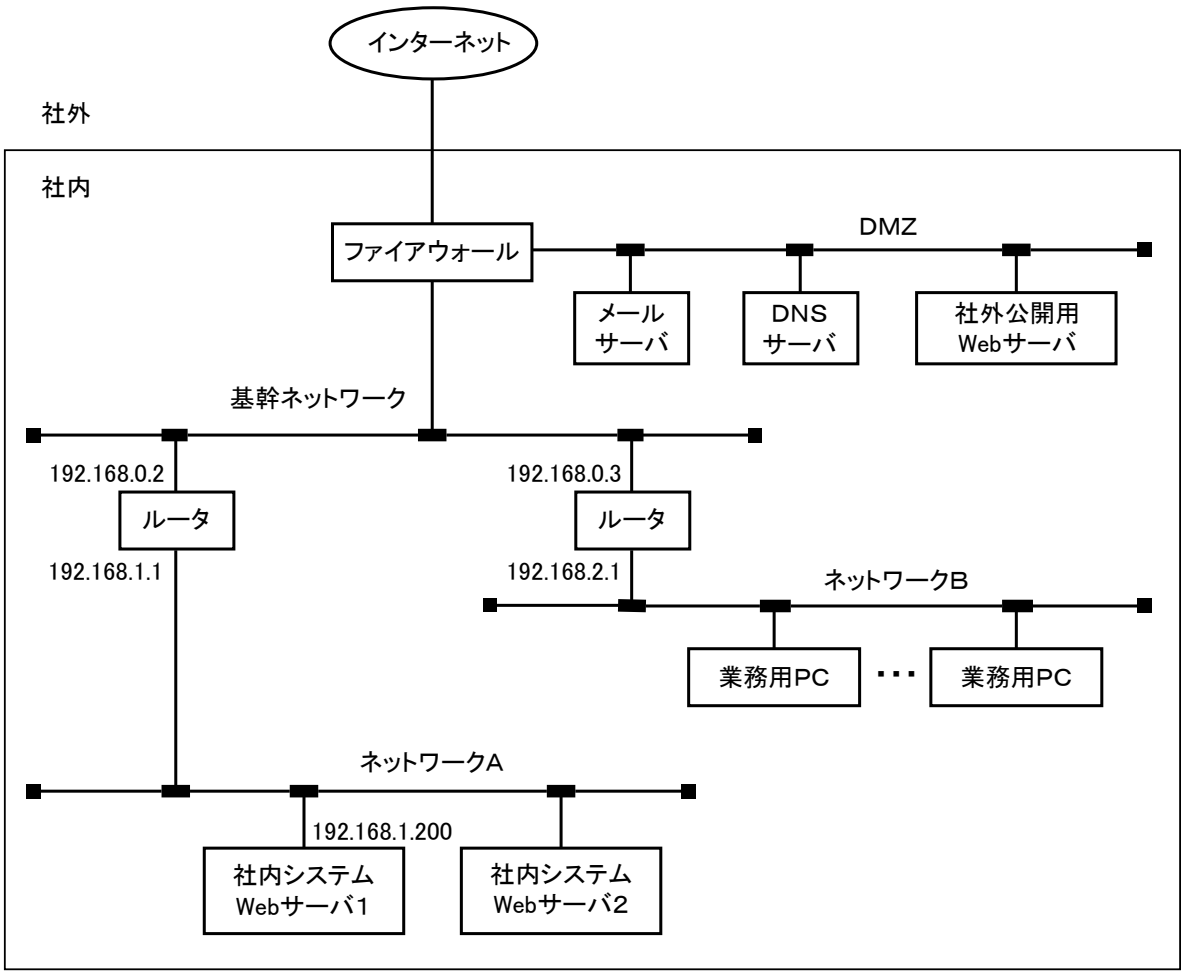
(10) の解答群

ア．装置Ｘを並列化する
イ．装置Ｙを並列化する
ウ．装置Ｚを並列化する
エ．装置Ｘと装置Ｙを共に並列化する
オ．装置Ｘと装置Ｚを共に並列化する
カ．装置Ｙと装置Ｚを共に並列化する
キ．装置Ｘ，装置Ｙおよび装置Ｚをすべて並列化する

問題３　次のネットワーク構築に関する記述を読み，各設問に答えよ。

J 社の現在のネットワーク構成を図に示す。DMZ には，メールサーバ，DNS サーバ及び社外公開用 Web サーバを設置している。また，ネットワーク A には，社内システムを稼働させる Web サーバを，ネットワーク B には，社員が通常業務を行うための業務用 PC を接続している。

ファイアウォールは，インターネットから基幹ネットワークに向けた通信と，基幹ネットワークからインターネットへ向けた通信を,すべて遮断している。したがって，業務用 PC から，社内にある社外公開用 Web サーバや，社内システム Web サーバへはアクセスできるが，社外の Web サーバへはアクセスできない。



注) 数字は各ルータ及び社内システムWebサーバ1の，各ネットワークでのIPアドレスである。

図　J 社の現在のネットワーク構成

＜設問１＞　次のIPアドレスに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

J社の各ネットワークに接続された機器のIPアドレスから，このネットワークはクラス［(1)］に設定されていることがわかるので，ネットワークAのサブネットマスクは［(2)］であることがわかる。

ネットワークAのネットワークアドレスとサブネットマスクを考慮すると，社内Webサーバ2に設定可能なIPアドレスは，次の表の中では6個のうち［(3)］個ある。

表　IPアドレス

192.168.0.4
192.168.0.255
192.168.1.1
192.168.1.2
192.168.2.0
192.168.2.2

また，ネットワークBの業務用PCを，部署ごとにさらにサブネット化することにした。部署数を最大5までとすると，業務用PCのサブネットマスクは［(4)］となり，部署ごとに設置できるホストの最大数は［(5)］台である。このとき，IPアドレスが192.168.2.130と［(6)］の業務用PCは，同じ部署に所属する。

ただし，ホスト部には，全てのビットが0または1の値は使用できないものとする。

(1) の解答群

ア．A　　イ．B　　ウ．C　　エ．D

(2)，(4) の解答群

ア．255.0.0.0　　イ．255.255.0.0
ウ．255.255.255.0　　エ．255.255.255.128
オ．255.255.255.192　　カ．255.255.255.224
キ．255.255.255.240　　ク．255.255.255.248

(3) の解答群

ア．1　　イ．2　　ウ．3　　エ．4　　オ．5　　カ．6

(5) の解答群

ア．14　　イ．16　　ウ．30　　エ．32　　オ．62　　カ．64

(6) の解答群

ア．192.168.2.80　　イ．192.168.2.100
ウ．192.168.2.120　　エ．192.168.2.140

＜設問２＞　次のDHCPサーバ及びプロキシサーバに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

J社は，業務用PCにIPアドレスなどのネットワーク情報を設定するために，DHCPを利用することにした。DHCPを利用する業務用PCは，DHCPサーバを見つけるためのメッセージをブロードキャストする。J社はDHCPのメッセージを中継する装置は設置しないので,業務用PCからのメッセージを受信するために,DHCPサーバは［(7)］に設置する必要がある。

また，業務用PCから社外のWebサーバへアクセスするために，プロキシサーバを設置することにした。プロキシサーバはクライアントからの要求に基づき．クライアントの代わりにWebサーバにアクセスし，Webサーバからの応答をクライアントに転送する。インターネットと基幹ネットワーク間の直接の通信は遮断したままにしておきたいので，プロキシサーバは［(8)］に設置する必要がある。

設置するプロキシサーバは,キャッシュサーバの機能を備えている。キャッシュサーバは，クライアントから要求されたWebページや画像などが，すでにキャッシュに格納されていれば(キャッシュにヒットすれば)，Webサーバに改めてアクセスせずに，キャッシュに格納されている内容をクライアントに送るので，応答時間の短縮が見込める。しかし，キャッシュにヒットしなければWebサーバにアクセスし，Webサーバからの応答をクライアントに転送するとともに，内容をキャッシュに格納するので，オーバヘッドが生じる。

キャッシュサーバを利用しないときの平均応答時間を100としたときに，キャッシュサーバ利用時の平均応答時間が，キャッシュにヒットしたときで35，ヒットしなかったときで110だとする。このとき，キャッシュのヒット率が［(9)］%以上であれば，キャッシュサーバ利用時の平均応答時間は，キャッシュサーバを利用しないときの平均応答時間の半分以下になる。

(7)，(8) の解答群

ア．DMZ　　イ．基幹ネットワーク
ウ．ネットワークA　　エ．ネットワークB

(9) の解答群

ア．40　　イ．50　　ウ．60　　エ．70　　オ．80　　カ．90

問題４　次のデータベースに関する記述を読み，各設問に答えよ。

Ｊホームセンターでは，売上管理にリレーショナルデータベースを使用している。

売上伝票

販売番号　07310　　受付日　20XX/7/5
顧客コード　0234
顧客名　M商店　　合計金額　21,430

商品コード	商品名	数量	単価	金額
B-CB	クーラーボックス	2	8,890	17,780
M-M3	木炭３kg	5	580	2,900
H-L8	保冷剤Ｌ	3	250	750

図１　売上伝票の例

売上伝票は，顧客からの１回の注文に対して作られ，顧客は１回の注文で１つ以上の商品を購入できる。また，同じ顧客から，１日に２回以上の注文を受ける場合もある。

販売番号は，1 回の注文ごとに割り当てられる番号で，売上伝票ごとに重複しない番号が自動的に付与される。

なお，値引きは発生しないものとする。

これらの管理で使用するテーブルは次のようになっている。下線の項目は主キーである。また，(FK) が付いている項目は外部キーである。

売上表（販売番号，販売年月日，顧客コード(FK)）

売上明細表（販売番号(FK)，商品コード(FK)，数量）

顧客表（顧客コード，顧客名）

商品表（商品コード，商品名，単価）

＜設問１＞　次の商品売上一覧作成に関する記述を読み，SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。

売上状況を分析するため，指定された期間の商品売上一覧を作成する。

商品売上一覧は，指定月の売上合計金額の多い順に表示する。ただし，売上合計金額が同じ場合は，売上数量の多い順に表示する。なお，指定月の開始日と終了日はホスト変数“:指定月開始日”と“:指定月終了日”に格納されているものとする。

［指定された期間の商品売上一覧］

```
SELECT  売上明細表.商品コード，商品名，SUM(単価 * 数量) AS 売上合計金額，
        SUM(数量) AS 売上数量
  FROM  売上表，売上明細表，商品表
 WHERE  [ (1) ]
   AND  売上明細表.商品コード ＝ 商品表.商品コード
   AND  販売年月日 BETWEEN :指定月開始日 [ (2) ] :指定月終了日
GROUP BY [ (3) ]
ORDER BY [ (4) ]
```

(1) の解答群

ア．売上表.顧客コード ＝ 顧客表.顧客コード
イ．売上表.商品コード ＝ 売上明細表.商品コード
ウ．売上明細表.販売番号 ＝ 売上表.販売番号
エ．商品表.商品コード ＝ 売上明細表.商品コード

(2) の解答群

ア．AND　　イ．FROM　　ウ．OR　　エ．TO

(3) の解答群

ア．売上明細表.商品コード
イ．売上明細表.商品コード，商品名
ウ．売上明細表.商品コード，商品名，売上合計金額
エ．売上明細表.商品コード，商品名，売上合計金額，売上数量

(4) の解答群

ア．売上合計金額，売上数量
イ．売上数量，売上合計金額
ウ．売上合計金額，売上数量 DESC
エ．売上合計金額 DESC，売上数量 DESC

＜設問２＞　次の注文金額の平均に関する記述を読み，SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。

指定された期間内で，１回に顧客が行う注文における合計金額の平均を求める。

［指定された期間に顧客が１回に注文する金額の平均］

```
SELECT  (5) / (6)
  FROM  売上表，売上明細表，商品表
 WHERE  (1)
   AND  売上明細表.商品コード ＝ 商品表.商品コード
   AND  販売年月日 BETWEEN :指定月開始日 (2) :指定月終了日
```

(5)，(6) の解答群

ア．AVG(単価 * 数量)　　イ．AVG(SUM(単価 * 数量))

ウ．COUNT(*)　　エ．COUNT(売上明細表.販売番号)

オ．COUNT(DISTINCT 売上明細表.販売番号)

カ．SUM(単価 * 数量)

＜設問３＞　次の割引に関する記述を読み，SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。

売上げを分析すると，季節商品の売上げが伸びていることが分かった。

そこで，さらに季節商品の売上げを伸ばすため，季節商品を割引商品として販売することにした。割引商品を購入したならば，2 個以上の購入があった場合に価格を 5%割引くことにする。

このため，新たに割引商品表を作成し，割引の対象となる季節商品を登録した。

割引商品表［商品コード(FK)］

１回の注文でどの程度割り引かれるのか，過去のデータを利用して割引商品を導入した場合の割引額を求める。

なお，割引額を求めるときに，１円未満は TRUNC 関数を使って切り捨てる。TRUNC 関数では，第 2 パラメータに 0 を設定することで，小数点以下の切捨てを行う。

```
SELECT  販売番号，TRUNC( SUM(単価 * 数量) * (7) , 0) AS 割引額
  FROM  売上明細表，商品表，割引商品表
 WHERE  (8)
   AND  売上明細表.商品コード ＝ 商品表.商品コード
GROUP BY (9)
(10)  SUM(数量) >= 2
```

(7) の解答群

ア. 0.05　　イ. 0.5　　ウ. 0.95　　エ. 5

(8) の解答群

ア. 売上明細表.商品コード ＝ 割引商品表.商品コード

イ. 売上明細表.販売番号 ＝ 割引商品表.商品コード

ウ. 商品表.商品コード ＝ 売上明細表.販売番号

エ. 商品表.顧客コード ＝顧客表. 顧客コード

(9) の解答群

ア. 販売番号

イ. 販売番号, SUM(単価*数量)

ウ. 販売番号, 売上明細表.商品コード

エ. 販売番号, 売上明細表.商品コード, SUM(単価*数量)

(10) の解答群

ア. AND　　イ. HAVING

ウ. ORDER BY　　エ. WHERE

問題５　次の利用者認証に関する各設問に答えよ。

クライアントからサーバへ接続する場合，セキュリティ上の必要性から利用者認証をする場合がある。利用者認証には様々な方法があるが，認証情報の盗聴や漏えいを防止するための方法も考えなければならない。

＜設問１＞　次の利用者 ID とパスワードによる認証方式に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

利用者はサーバに利用者 ID とパスワードを送信し，サーバ側で登録してある利用者 ID とパスワードかを判断して認証を行うものである。

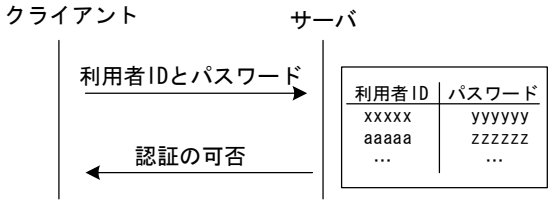


図１　利用者 ID とパスワードによる認証

パスワードには推測されにくい文字を利用し，桁数を増やすなどしてパスワードの強度を高める必要がある。

ここで，パスワードを発見するために，″aaa″，″aab″，″aac″，…，″zzz″のように，1 文字ずつ入れ替える総当たり方式で探索する場合を考える。

英小文字だけの 4 文字を使用して作成したパスワードを総当たり方式で発見するのにかかる時間が最大で T とした場合を考える。

英小文字と英大文字を使用した場合，1 文字当たりの選択肢は 2 倍になるので，4 文字で作成したパスワードは，発見に要する時間が最大で［　(1)　］となる。

なお，サーバ側では，［　(2)　］仕組みを導入して，総当たり方式によるパスワードの発見を防ぐ必要がある。

さらに，パスワードが盗聴されない工夫も必要である。パスワードが盗聴される要因として，パスワードを入力する現場を盗み見られる場合や，不正プログラムによりキーボードから入力した文字を外部に送信する［　(3)　］がある。

(1) の解答群

ア．2×T　　イ．8×T　　ウ．16×T　　エ．26×T

(2) の解答群

ア．暗号化通信を行う
イ．指定された IP アドレスからの接続だけを許可する
ウ．定期的にパスワードを変更する
エ．連続して認証に失敗した利用者 ID を使用不可にする

(3) の解答群

ア．キーロガー　　イ．ゼロディアタック
ウ．バックドア　　エ．ポートスキャン

＜設問２＞　次のワンタイムパスワードに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

一度だけ有効なパスワードをワンタイムパスワードと呼ぶ。ワンタイムパスワードの生成にはいくつかの方法があるが，ここでは２つの方法について検証する。

［時刻同期方式］

トークンと呼ばれるパスワード生成器を利用するもので，トークンには時刻をもとに生成したパスワードが表示される。サーバにもトークンと同じ仕組みでパスワードを生成する仕組みが存在するので，利用者から送信されたパスワードとサーバで生成したパスワードを比較して認証の可否を判断する。

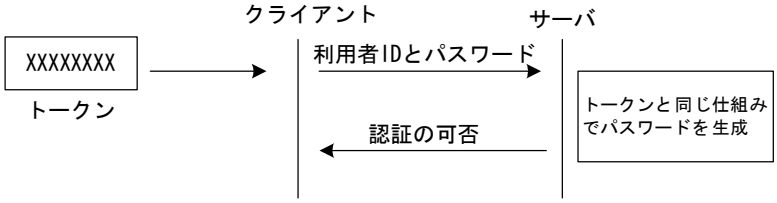


図２　時刻同期方式による認証

この方式の場合，［　(4)　］必要がある。

トークンは，おもに１分間隔でパスワードを生成するが，トークンとサーバでズレが生じる可能性がある。サーバでは，このズレに対して許容範囲を設定している。例えば,前後１分ずれた場合のパスワードと一致すれば認証を許可するようにしている。

(4) の解答群

ア．DHCP サーバから IP アドレスを再取得する
イ．あらかじめトークンとサーバの時刻を同期させる
ウ．トークンとサーバ間で自動認証を行う
エ．利用者 ID を登録しているテーブルの再構築する

［S/Key 方式］

回数を示す番号（シーケンス番号）やシードと呼ばれる値などをもとに一方向ハッシュ関数に入力した結果をパスワードとして用いる方式である。

S/Key 方式は，次のような手順で行う。

＜事前準備＞

① 利用者は利用者 ID とパスフレーズをサーバに登録する。

② サーバはランダムに生成したシードとパスフレーズを一方向ハッシュ関数に入力して 1 回目のワンタイムパスワードを生成する。2 回目以降は，1 回前のワンタイムパスワードをシードとして一方向ハッシュ関数に入力して生成する。

一方向ハッシュ関数を H，パスフレーズを p，ランダムに生成したシードを r とすれば，n 回目のワンタイムパスワードは次のように表現できる。

$$\text{n 回目のワンタイムパスワード} = \underbrace{H(p,\ H(p,\ H(\cdots,\ H(p,\ H(p,\ r))\cdots)))}_{\text{n 回}}$$

生成したワンタイムパスワードは，シーケンス番号とともに記録する。

＜認証の手順＞

① クライアントからサーバへ利用者 ID を送信する。

② サーバからシーケンス番号（n-1）とシードをクライアントに送信する。なお，シーケンス番号はアクセスするたびに 1 ずつ増加されてサーバに記録される。

③ クライアントは，一方向ハッシュ関数にパスフレーズとサーバから送られてきたシードを入力してワンタイムパスワードを生成し，サーバへ送る。

④ クライアントから受け取ったワンタイムパスワードとパスフレーズを一方向ハッシュ関数に入力して n 回目のワンタイムパスワードを生成し，登録してある n 回目のワンタイムパスワードと比較して認証の可否を判断する。

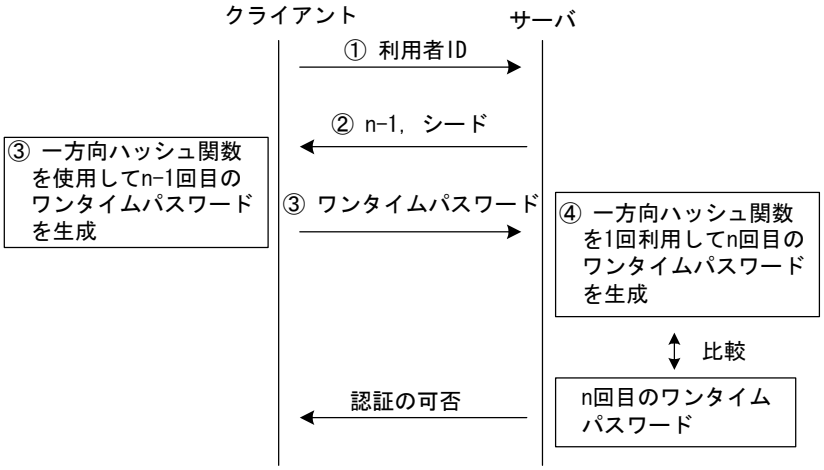


図３　S/Key による認証

ここで，認証の手順②～④を検証する。

なお，サーバ側で記録しているワンタイムパスワードとパスフレーズおよびシードは，図４のようになっているものとする。また，サーバとクライアントで同じハッシュ関数を用いる。

パスフレーズ 0000

シード 1111

シーケンス番号	ワンタイムパスワード
⋮	⋮
29	2222
30	3333
31	4444
⋮	⋮

図４　サーバに登録されている情報

認証手順	検証内容
②	30 回目の認証を行う場合，認証手順②でサーバからクライアントに送信されるシーケンス番号は 29 である。
③	クライアントの一方向ハッシュ関数で生成するワンタイムパスワードのもとになる値は 0000 と［　(5)　］であり，一方向ハッシュ関数を 29 回利用してワンタイムパスワードを生成する。正しい一方向ハッシュ関数を用いていれば，サーバに送信される値は［　(6)　］である。
④	サーバが受け取ったワンタイムパスワードとパスフレーズを一方向ハッシュ関数に入力して返された値が［　(7)　］であれば，認証が許可される。

この方法では，クライアントとサーバ間でやりとりされる利用者 ID，パスフレーズ，シーケンス番号，シードが盗聴されたとしても［　(8)　］が漏えいしない限り第三者が認証されることはない。

(5) ～ (7) の解答群

ア．29　　イ．30　　ウ．31　　エ．0000

オ．1111　　カ．2222　　キ．3333　　ク．4444

(8) の解答群

ア．n-1 回目のワンタイムパスワード

イ．n 回目のワンタイムパスワード

ウ．一方向ハッシュ関数

エ．サーバに登録しているワンタイムパスワードの数